

Patent
62478-9100

IN THE CLAIMS:

1 1-15. (Cancelled)

1 16. (Original) A file encryption apparatus that encrypts a plaintext to generate a
2 ciphertext and stores the ciphertext into a memory unit thereof, the file management apparatus
3 comprising:
4 a key storage medium storing key information beforehand;
5 registration means for receiving an input of a password, encrypts the key
6 information using the received password to generate an encrypted key, and writes the generated
7 encrypted key to the memory unit; and
8 encryption unit means for encrypting a plaintext using a file key to generate a
9 ciphertext, encrypting the file key using the key information to generate an encrypted file key,
10 and writing the ciphertext in association with the encrypted file key, to the memory unit.

1 17. (Original) A file decryption apparatus that stores the ciphertext and the encrypted
2 file key generated by the file encryption apparatus of Claim 16, in association with each other, in
3 a memory unit thereof, and decrypts the ciphertext, the file decryption apparatus comprising:
4 a key storage medium storing key information beforehand;
5 switch means
6 (a) including first key obtaining means for receiving an input of a password
7 and decrypting the encrypted key using the received password to generate key information, and
8 second key obtaining means for reading the key information from the key storage medium, and
9 (b) obtaining the key information by one of the first key obtaining means and
10 the second key obtaining means; and

Patent
62478-9100

11 decryption means for decrypting the encrypted file key using the obtained key
12 information to generate a file key, and decrypts the ciphertext using the file key to generate a
13 decrypted text.

1 18-43. (Cancelled)

Please add the following newly drafted Claims 44-60.

1 44. (New) The file encryption apparatus of Claim 16, wherein the registration means
2 further receives an input of a user identifier that identifies a user, and writes the user identifier in
3 association with the encrypted key, to the memory unit.

1 45. (New) The file encryption apparatus of Claim 16, wherein the registration means
2 further writes the key information and/or authentication information in association with the
3 encrypted key, to the memory unit,

4 the encryption means further writes the encrypted key, the key information, and/or
5 authentication information in association with the ciphertext, to the memory unit.

1 46. (New) The file encryption apparatus of Claim 16, wherein the registration means
2 writes the encrypted key to the memory unit that is a portable storage medium.

1 47. (New) The file encryption apparatus of Claim 16, further comprising:
2 deletion means for deleting the encrypted key that has been written to the memory unit.

Patent
62478-9100

1 48. (New) The file encryption apparatus of Claim 16, further comprising:

2 deletion means for deleting the encrypted key that has been written to the memory
3 unit,

4 wherein the registration means further receives an input of a new password, encrypts
5 the key information using the new password to generate a new encrypted key, and writes the
6 generated new encrypted key to the memory unit.

1 49. (New) The file encryption apparatus of Claim 16, wherein the key storage
2 medium stores new key information beforehand, instead of the key information,

3 the registration means receives the input of the password and decrypts the encrypted
4 key using the password to generate key information,

5 the encryption means decrypts the encrypted file key using the key information to
6 generate a file key, encrypts the file key using the new key information to generate a new
7 encrypted file key, and writes the new encrypted file key over the encrypted file key in the
8 memory unit, and

9 the registration means encrypts the new key information using the password to
10 generate a new encrypted key and writes the new encrypted key over the encrypted key in the
11 memory unit.

1 50. (New) The file encryption apparatus of Claim 49, wherein the registration means
2 further receives an input of a user identifier that identifies a user,

Patent
62478-9100

3 the encryption means further writes the user identifier in association with the ciphertext
4 and the encrypted file key, to the memory unit, and

5 the encryption means retrieves the encrypted file key that is associated with the user
6 identifier in the memory unit and generates a file key from the retrieved encrypted file key.

1 51. (New) The file encryption apparatus of Claim 49, wherein the encryption means
2 further writes encryption information in association with the ciphertext and the encrypted file
3 key, to the memory unit, the encryption information indicating that the plaintext has been
4 encrypted, and

5 the encryption means retrieves the encrypted file key that is associated with the
6 encryption information in the memory unit, and generates a file key from the retrieved encrypted
7 file key.

1 52. (New) The file encryption apparatus of Claim 49, wherein the registration means
2 further receives an input of a user identifier that identifies a user,

3 the encryption means further writes the user identifier in association with a file
4 identifier that identifies the ciphertext and the encrypted file key, as a unified file, to the
5 memory unit, and

6 the encryption means extracts the file identifier that is associated with the user
7 identifier from the unified file, specifies the encrypted file key identified by the extracted file
8 identifier, and generates a file key from the specified encrypted file key.

Patent
62478-9100

1 53. (New) The file encryption apparatus of Claim 49, wherein the encryption means
2 further writes encryption information in association with a file identifier that identifies the
3 ciphertext and the encrypted file key, as a unified file, to the memory unit, the encryption
4 information indicating that the plaintext has been encrypted, and the encryption means extracts
5 the file identifier that is associated with the encryption information from the unified file,
6 specifies the encrypted file key identified by the extracted file identifier, and generates a file
7 key from the specified encrypted file key.

1 54. (New) The file encryption apparatus of Claim 16, wherein the encryption means
2 further writes the encrypted key in association with the ciphertext and the encrypted file key,
3 to the memory unit.

1 55. (New) The file encryption apparatus of Claim 54, wherein the encryption means
2 further receives an input of an indication, the indication showing whether the encrypted key
3 and the ciphertext are to be written in association with each other to the memory unit, and
4 writes, when the indication shows that the encrypted key and the ciphertext are to be written
5 in association with each other, the encrypted key in association with the ciphertext, to the
6 memory unit.

1 56. (New) The file encryption apparatus of Claim 54, wherein the registration means
2 writes the generated encrypted key to the key storage medium instead of to the memory unit.

Patent
62478-9100

1 57. (New) The file decryption apparatus of Claim 17, wherein the file encryption
2 apparatus further receives an input of a user identifier that identifies a user, and writes the
3 user identifier in association with the encrypted key, to the memory unit, and

4 the first key obtaining means further receives an input of the user identifier and
5 decrypts the encrypted key that is associated with the user identifier.

1 58. (New) The file decryption apparatus of Claim 17, wherein the file encryption
2 apparatus further writes the key information and/or authentication information in association
3 with the encrypted key, to the memory unit, and further writes the encrypted key, the key
4 information, and/or authentication information in association with the ciphertext, to the
5 memory unit,

6 the first key obtaining means checks, using the authentication information, whether the
7 encrypted key has been altered or not, when the encrypted key that is associated with the
8 authentication information is decrypted, and the decryption means checks, using the
9 authentication information, whether the ciphertext has been altered or not, when the ciphertext
10 that is associated with the authentication information is decrypted.

1 59. (New) The file decryption apparatus of Claim 17, wherein the file encryption
2 apparatus writes the encrypted key to the memory unit that is a portable storage medium, and

3 the first key obtaining means decrypts the encrypted key that has been written to the
4 memory unit that is the portable storage medium.

Patent
62478-9100

- 1 60. (New) The file decryption apparatus of Claim 17,
- 2 wherein the file encryption apparatus further writes the encrypted key in association with
- 3 the ciphertext and the encrypted file key, to the memory unit, and
- 4 the first key obtaining means decrypts the encrypted key that is associated with the
- 5 ciphertext and the encrypted file key.